UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/419,828	10/14/1999	DON VAN DYKE	M-7084-US	1859

23418 7590 09/07/2005

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/419,828
Filing Date: October 14, 1999
Appellant(s): DYKE ET AL.

Patrick B. Law, Reg. No. 41,549
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 7/11/05 appealing from the Office action mailed 2/8/05.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect.

The amendment after final rejection filed on July 7, 2005 has been entered.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,088,800	Jones et al.	7-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 3-13 and 15-23 are rejected under 35 U.S.C. 102 as being anticipated by Jones et al. This rejection is set forth in the prior Office action dated 2/8/05 and repeated here for convenience.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 3-13, and 15-21 are rejected under 35 U.S.C. 102(e) as being anticipated by U. S. patent 6,088,800 granted to Jones et al.

Regarding claim 1, Jones meets the claimed limitations as follows:

"A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations wherein said computer system further comprises a register file providing operands to said arithmetic logic unit, and

wherein said register file includes general purpose registers." see column 6, lines

3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 3, Jones meets the claimed limitations as follows: "The method of claim 1, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 4, Jones meets the claimed limitations as follows: "The computer system of Claim 3, wherein said datum is 64 bits long and said subkey is 48 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14. See sample code in column 17, where A (first datum is loaded in register 1), B (second datum loaded in register 2) and K (subkeys computed and stored in advance in order to XOR with the expanded group) (see column 17, lines 1-14).

Regarding claim 5, Jones meets the claimed limitations as follows: "The computer system of Claim 3, wherein said first and second portions each contain one-half number of bits of said datum." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 6, Jones meets the claimed limitations as follows: "The computer system of Claim 5, wherein each of said first and second portions is 32

bits long." see column 6, lines 3-13; column 7, lines 15-38., column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 7, Jones meets the claimed limitations as follows: "The computer system of Claim 3, wherein said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 8, Jones meets the claimed limitations as follows: "The computer system, of Claim 7, wherein a bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers." see column 6, lines 3-13, column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 9, Jones meets the claimed limitations as follows: "The computer system of Claim 8, wherein said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 10, Jones meets the claimed limitations as follows:

"The computer system of Claim 1, further comprising a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operating in parallel with said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 11, Jones meets the claimed limitations as follows:

"The computer system of Claim 1, wherein said logic circuit further comprises a circuit for selecting a subkey from a key." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 12, Jones meets the claimed limitations as follows:

"The computer system of Claim 11, wherein said key is 56 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 13, Jones meets the claimed limitations as follows:

"A process for performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

providing a logic circuit in an arithmetic logic unit, and

performing expansion permutation, S-box substitution and P-box permutation and associated XOR operations in said logic circuit, and storing operands in a register file;

and providing said operands to said logic circuit; wherein said register file includes genera! purpose registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 15, Jones meets the claimed limitations as follows: "The process of Claim 13, further comprising: storing operands in a register file; and providing said operands to said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 16, Jones meets the claimed limitations as follows: "The process of Claim 15, further comprising: storing a first portion of a datum for said encryption or decryption in first register in said register file; storing a second portion of said datum for said encryption or decryption in second register in said register file, and storing a subkey for said encryption or decryption in third register in said register file." see column 6, lines 3-13., column 7, lines 15-38., column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 17, Jones meets the claimed limitations as follows: "The process of Claim 16, further comprising storing operands of an instruction executing one round of said DES algorithm in said first, second and third registers using said logic circuit and said shift circuit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 18, Jones meets the claimed limitations as follows: "The process of Claim 17, further comprising providing said results as input to said logic circuit without first being written back to said first, second and third registers." see

column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 19, Jones meets the claimed limitations as follows: "The process of Claim 13, further comprising selecting a subkey from a key for said DES algorithm in a second logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 20, Jones meets the claimed limitations as follows: "The process of Claim 19, further comprising operating said second logic circuit in parallel with said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 21, Jones meets the claimed limitations as follows: "The process of Claim 13, further comprising selecting a subkey from a key using a key select circuit in said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 22, Jones meets the claimed limitations as follows: "A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising: an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations;

wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and

wherein said register file includes general purpose registers to store at least two

of attributes parameters datapath, control, Li's, Ri's, and subkeys Ki's." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 23, Jones meets the claimed limitations as follows: "The method of claim 1, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a second portion of said datum and a third register for storing a subkey." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14. See sample code in column 17, where A (first datum is loaded in register 1); B (second datum loaded in register 2) and K (subkeys computed and stored in advance in order to XOR with the expanded group) (see column 17, lines 1-14).

(10) Response to Argument

In general, appellant's arguments fail to consider the full teachings of the reference in light of the knowledge generally available to one of ordinary skill in the art.

First, Appellant argues the system of Jones is a dedicated single purpose processor whose instruction set is optimized for common encryption algorithms and is distinguished from a general-purpose processor as shown in column 10, lines 20-29 of the Jones reference. More specifically, appellant states, "Jones distinguishes that his disclosed encryption processor is different from [general purpose processing] by stating that "[general purpose processing systems]" **are not required for encryption**, an embodiment of the present invention uses a simpler linear arrangement of the (processing elements) with much less switching circuitry (Jones, col. 10, lines 20-29)".

Appellant's view of the section of Jones given above is not correct. First, this section shows Jones chooses a simpler linear arrangement embodiment because **the switching matrix** is not needed for encryption and not for the reason suggested in appellant's statement. The section shows a switching matrix is needed in a multiprocessing architecture in order for data to be switched from one processing elements to another (see Figure 5, elements 74 and 76). Second, this section of Jones does not suggest that a general-purpose processor cannot be used to accomplish his objective but rather, most proposed multiprocessor architectures are designed for general-purpose processing as the processing elements communicate between one another. Also, nowhere in the quoted section does it suggest the simpler arrangement is limited to specific purpose registers.

Next, appellant argues Jones does not teach or suggest "general purpose registers" but rather specific purpose registers used in a dedicated encryption/decryption processor. Appellant relies on the same section given below along with column 3, lines 33-35 to support the assertion that Jones only suggests or teach specific purpose registers. However, Jones does state, in column 3, lines 35-40, "The present invention realizes the advantages of both hardware and software approaches. Since the processor is a programmable processor, any encryption algorithm may be implemented, contrary to a hardware implemented encryption processor which is dedicated to executing only one algorithm. The above quoted statements would lead one of ordinary skill in the applied art to conclude that the processor is not dedicated to executing only one algorithm and that the processor uses

the same architecture (registers) regardless of the type of encryption algorithm been employed at a particular point in time. Also, Jones teaches at column 7, lines 15-25, the register file contains (8-16) 32 bit registers, where these registers are used in conjunction with an instruction from the processing element's memory to complete one round of an encryption algorithm. The registers can be used as an operand to any instruction which allows them to act as a general purpose register (i.e. a register that is not specifically addressed for one purpose). Since the same architecture is being used, the registers are not used for only a specific purpose but are addressable depending on the type of instruction being used during process of the chosen encryption algorithm.

Further, even if one were to construe that the registers in Jones were not general purpose registers but rather dedicated special purpose registers, appellant's claimed language has failed to clearly distinguish the claimed general purpose registers from the registers in Jones. Appellant's arguments concerning the general purpose registers merely characterize the use of general purpose registers as they are known to be addressable for specific tasks, like serving as an accumulator or as an index register. The arguments are mainly based on information found in the specification and although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Unfortunately none of the claims recite language that makes a clear distinction between the registers in Jones and the appellant's claimed registers. Appellant's claim language simply requires a register file to include general purpose registers that can store at least two attribute parameters, such as L_i and R_i (the left half

of the input and the right half of the input), that are used in the process of performing an encryption with the DES algorithm. Jones shows in Figure 14, locations A and B are each used to store one-half of the 64-bit plaintext input. The locations (A and B) are registers used to store the L_i and R_i values of the 64-bit plaintext input (see column 15, lines 10-14; column 16, line 62 to column 17, line 9). Therefore, Jones' registers function in the same manner as appellant's registers when performing an encryption process.

As for the dependent claims, the reference does not specifically state a first register, second register, or third register, however, it is clear the system described in the reference uses at least 8 registers, some of which can be programmed to store data according to the encryption algorithm being applied. Further, Jones discloses performing a DES encryption process where the plaintext input (datum) is 64-bits long (see column 16, lines 62-64) and states the subkeys are a function of the processing element and the single 56-bit key (see column 16, line 67 to column 17, line 2).

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Matthew B. Smithers

August 30, 2005

Conferees:

Gilberto Barron SPE2132

Emmanuel Moise. SPE 2137